

# **Toolset On-line User Guide:**

# **User Administration**

---

**HP/ElectraLink DTS**

**Table of Contents**

|            |                                               |           |
|------------|-----------------------------------------------|-----------|
| <b>1</b>   | <b>DOCUMENT AUTHORISATION.....</b>            | <b>3</b>  |
| <b>1.1</b> | <b>The User Access Summary.....</b>           | <b>5</b>  |
| <b>1.2</b> | <b>The User Administration Tool.....</b>      | <b>7</b>  |
| 1.2.1      | User List.....                                | 7         |
| 1.2.2      | Searching for User Accounts .....             | 8         |
| 1.2.3      | Sorting User Accounts .....                   | 8         |
| 1.2.4      | Creating a New User .....                     | 8         |
| 1.2.5      | Changing User Details or Password .....       | 9         |
| 1.2.6      | Deleting a User .....                         | 10        |
| 1.2.7      | Defining User Access Levels.....              | 10        |
| 1.2.8      | Flow Access.....                              | 15        |
| <b>1.3</b> | <b>Automated Password Reset Facility.....</b> | <b>18</b> |
| 1.3.1      | Password Reset Request .....                  | 18        |

# 1 DOCUMENT AUTHORISATION

| DOCUMENT TITLE                                  | ISSUE | DATE           |
|-------------------------------------------------|-------|----------------|
| HP/ElectraLink DTS – Toolset On-line User Guide | 1.0   | 15th June 2011 |

|                          | NAME          | SIGNATURE | DATE |
|--------------------------|---------------|-----------|------|
| AUTHOR(S)                | Gareth Hughes |           |      |
| REVIEWER(S)              |               |           |      |
| HP                       | Alan McDonald |           |      |
|                          |               |           |      |
|                          |               |           |      |
|                          |               |           |      |
|                          |               |           |      |
|                          |               |           |      |
| ElectraLink              | Mark Pearce   |           |      |
|                          |               |           |      |
|                          |               |           |      |
|                          |               |           |      |
|                          |               |           |      |
|                          | NAME          | SIGNATURE | DATE |
| ON BEHALF OF HP          |               |           |      |
| ON BEHALF OF ELECTRALINK |               |           |      |



## 2 THE USER ACCESS SUMMARY

This function allows all users to view a summary of the access levels that has been assigned to them.

To navigate to this function, from the Menu, click  **My Settings** followed by  **Access**. An example screen is shown below:

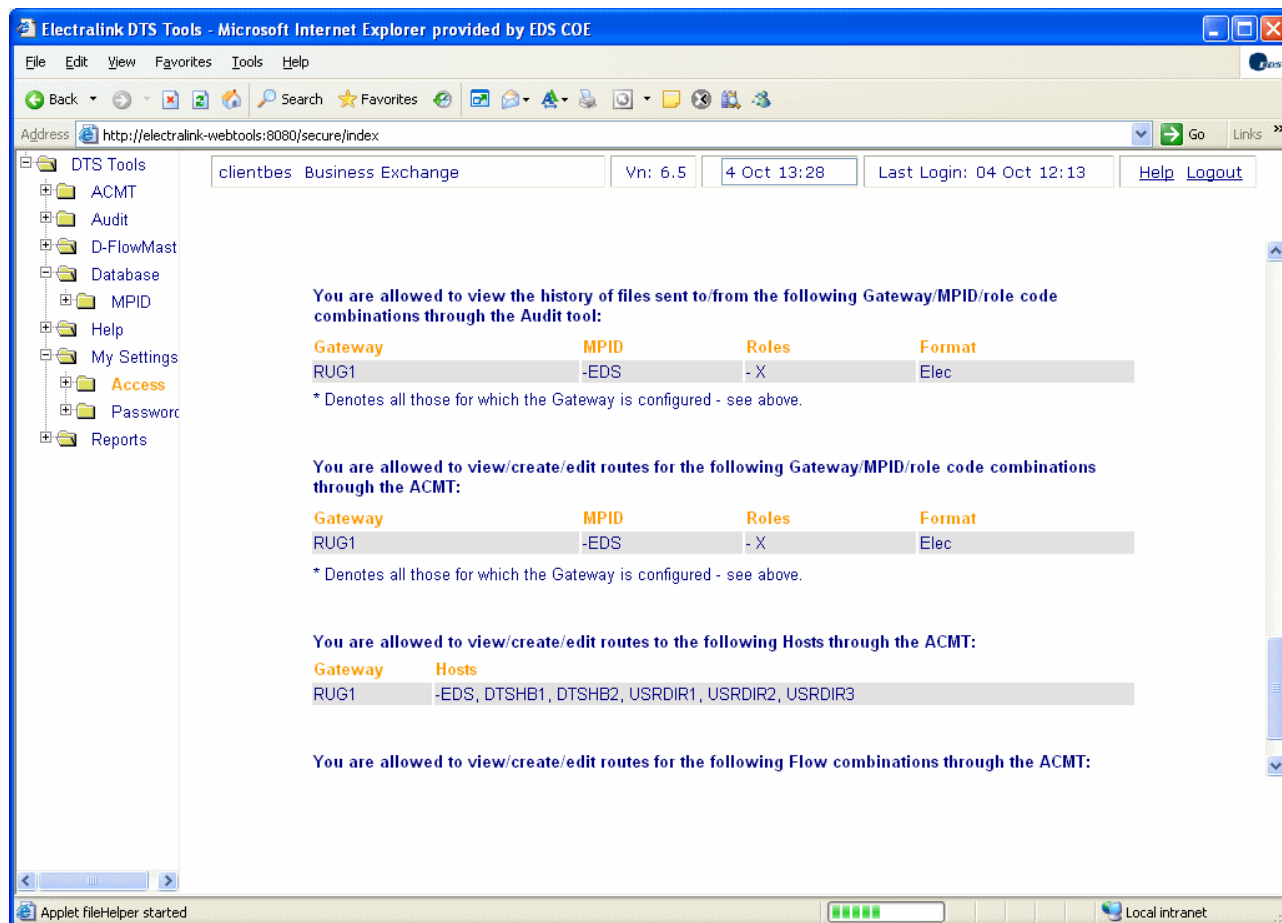


**Figure 1-1 User access Summary**

The summary displays the access levels granted to the logged-on user, specifically: MPID/Role, Gateways, Flows and Toolset Commands.

Note that the asterisk (\*) character denotes full access. An asterisk under the MPID heading, for example, indicates that the user may access all MPIDs (and any MPIDs added at a later date). An asterisk in the Roles column indicates access to all Roles associated with the corresponding MPID (plus any associated in the future) .

A user's access profile determines the functionality and data that is available to that user within the toolset. The effect of the various levels is as follows:

**Command Privilege:** Only those commands granted to the user will appear on the Toolset menu for selection.

**MPID/Role, Gateway, and Flow Range:** All information displayed or entered within the toolset is restricted in line with these user access levels.

Note that Gateway access is granted separately for ACMT and Audit. For ACMT the access indicates those gateways for which the user can configure Routes. For Audit, the access indicates those gateways (where the Gateway is the file sender or file receiver) for which the user may view Audit information.



### 3 THE USER ADMINISTRATION TOOL

The User Administration Tool enables authorised users to manage the accounts of users within their user group. If you wish to manage user accounts for users in your organisation, contact the ElectraLink helpdesk (on 020 7432 3012 or [helpdesk@electralink.co.uk](mailto:helpdesk@electralink.co.uk)) and request a user group be created for your organisation. The helpdesk will need to know the IDs of any existing user accounts to be added to the group and which user or users are to be authorised to manage the group. We also recommend you request a new account for user administration if users within your organisation currently share one account for WebTools access. Once you have created accounts for individual users within your organisation, the shared account should be deleted.

#### 3.1 USER LIST

The user list displays the users that are currently assigned to your user group.

To navigate to this display, click  **User** on the Menu.

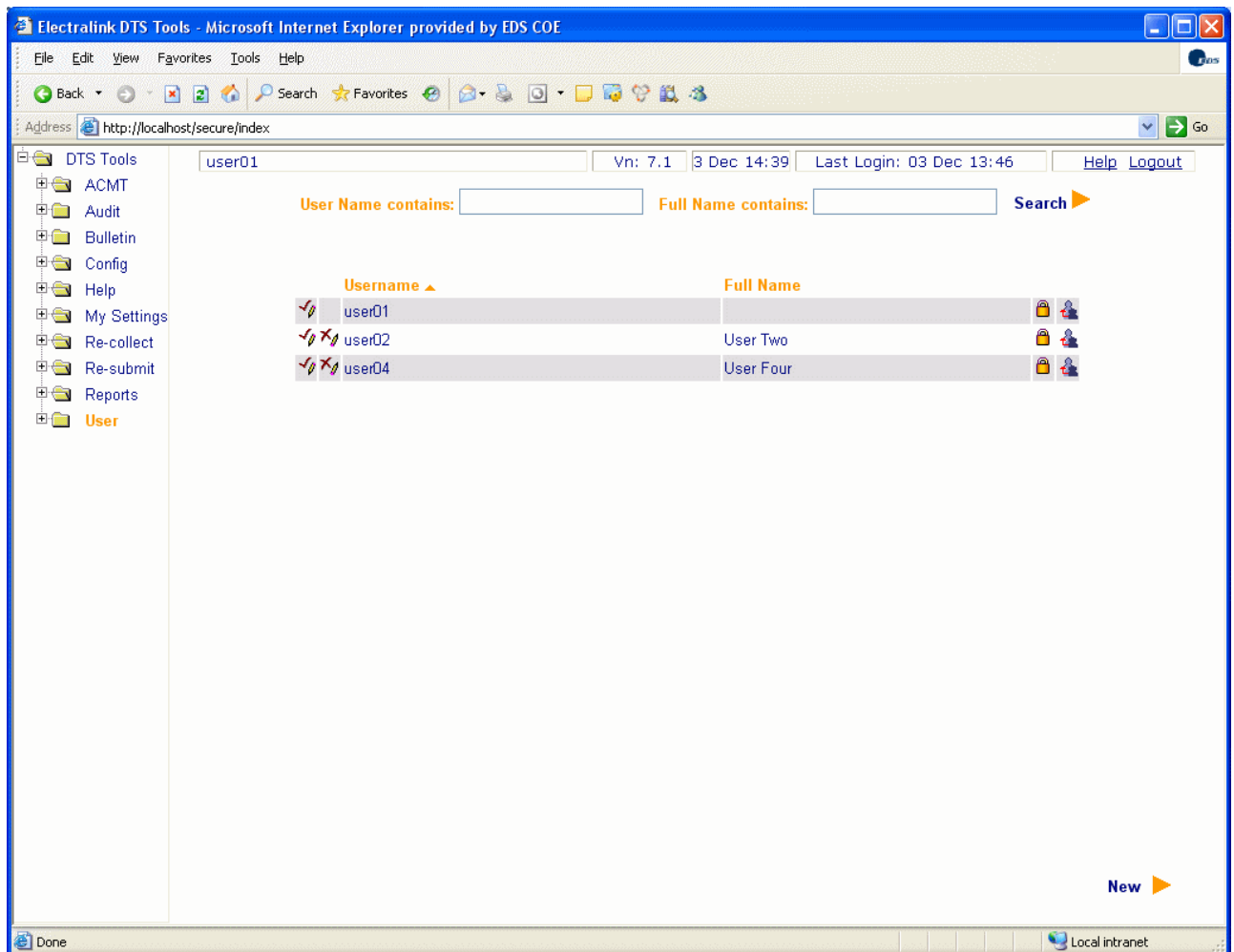


**Figure 1-1 User List**

From this display you can:

- Click on  to modify the first name, last name or description of the user; make the account inactive (preventing the user from logging in) or change the user's password.
- Click on  to delete the user account completely.
- Click on  to modify the user's privileges.
- Click on  to create a new user account, giving it the same privileges as this user.

- Click on **New**  to create a new user account without any privileges (these need to be defined afterwards).
- Click on **Search**  to find accounts that contain specified string of characters in the username or full name.

Inactive accounts are shown greyed-out.

## 3.2 SEARCHING FOR USER ACCOUNTS

To search for accounts which have a known string of characters in their username and/or in their full name, enter the character string into the appropriate search field ('User Name contains:' or 'Full Name contains:') and then click **Search** .

The search is case sensitive so you must use the correct capitalisation. For example, if you have a user account with a username of 'Tom', this will be found if you enter 'To' in the 'User Name contains:' search field, but will not be found if you enter 'to'.

An account must satisfy both search criteria to be displayed in the search results.

To display all accounts, leave both fields blank and click search. (This is the default behaviour on entry to this screen).

## 3.3 SORTING USER ACCOUNTS

User accounts may be ordered in ascending or descending username or full name order. By default, user accounts are ordered in ascending username order.

The order in which the user accounts are displayed is indicated by a small orange arrow on the right of the title of the column on which the data is ordered. An upward pointing arrow indicates the data is sorted in ascending order, and a downward pointing arrow indicates the data is sorted in descending order.

Clicking on the column showing the arrow will reverse the sort order on that column. Clicking on the a column not showing the arrow will sort the results on that column, in ascending order.

## 3.4 CREATING A NEW USER

After clicking **New**  on the User List (see above) the following form is displayed.

**Figure 2-2 Creating a new user**

The user name, password and confirm password fields are mandatory; the First Name, Last Name and description are optional.

User names beginning 'eds' or 'test', or user names where the second character is a 'z' are reserved for HP use.

If the 'Account Active' option is checked, the user will be able to login (once the account has been created) with the supplied username and password. It is your responsibility as User Administrator to supply your user with the username and password.

Conversely, users are unable to login to their accounts if the 'Account Active' option is un-checked.

To create the account click on **Save** ►.

To abort, click on **Cancel** ►.

### 3.5 CHANGING USER DETAILS OR PASSWORD

After clicking  on the User List (see above) the following form is displayed, showing the current details for the user.

**Figure 2-3 Modifying user details or password**

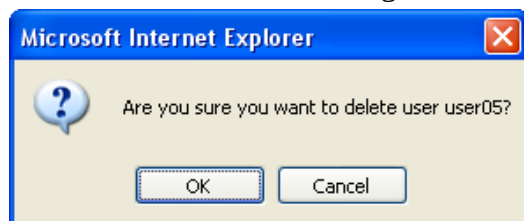
From this page, you may change the user's First Name, Last Name or Description. You may also activate or de-activate the account, and/or change the user's password.

To make the changes click on **Save** ➤.

To abort, click on **Cancel** ➤.

### 3.6 DELETING A USER

After clicking  on the User List (see above) you will be prompted for confirmation that you want to delete this user account. E.g.



Deleting the account permanently removes the account and all associated access controls from the DTS database, so the account cannot be restored after confirmation has been given.

### 3.7 DEFINING USER ACCESS LEVELS

After clicking  on the User List (see above) the following page is displayed, showing the current access levels for the user.

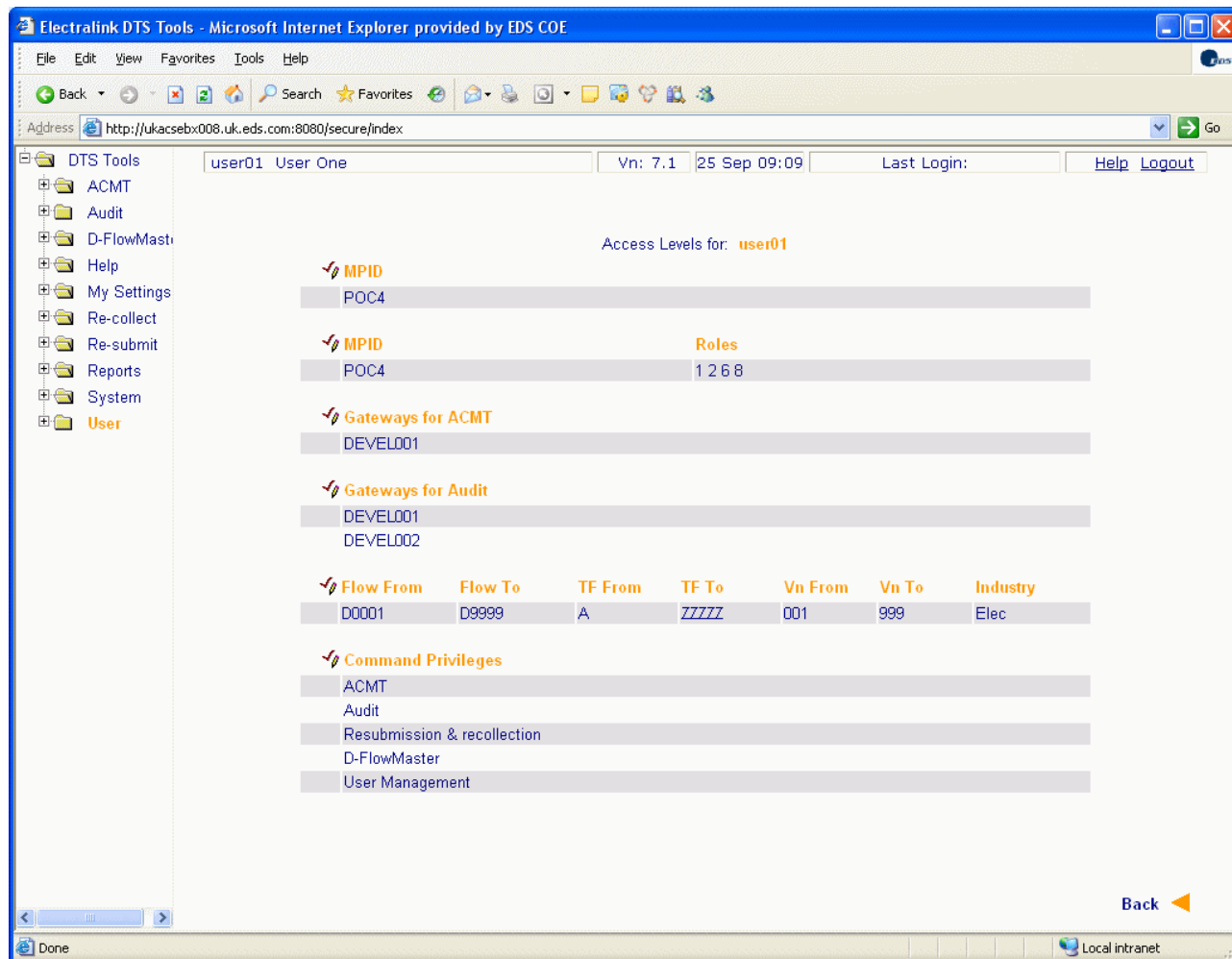


**Figure 2-4 Viewing user access levels**

The first table identifies the MPIDs that the user can access in the ACMT, Audit, Re-submission and Re-collection tools.

The second table identifies the Roles that the user can access in the ACMT, Audit, Re-submission and Re-collection tools. An asterisk (\*) in this table indicates that access is granted to all permissible values.

The third table identifies the gateways that the user can access in the ACMT.

The fourth table identifies the gateways that the user can access in the Audit, Re-submission and re-collection tools.

The fifth table identifies the range of flows the user can access in the ACMT.

The last table identifies those tools within the tool-set that the user can access.

From this page you can click on any of the  icons along side each of the tables to set-up or amend the corresponding user privileges.

Click on **Back**  to return to the User List.

### 3.7.1 Tool Access

After clicking on the  at the side of the last table on the user access levels display (see Defining User Access Levels above) the following page is displayed.

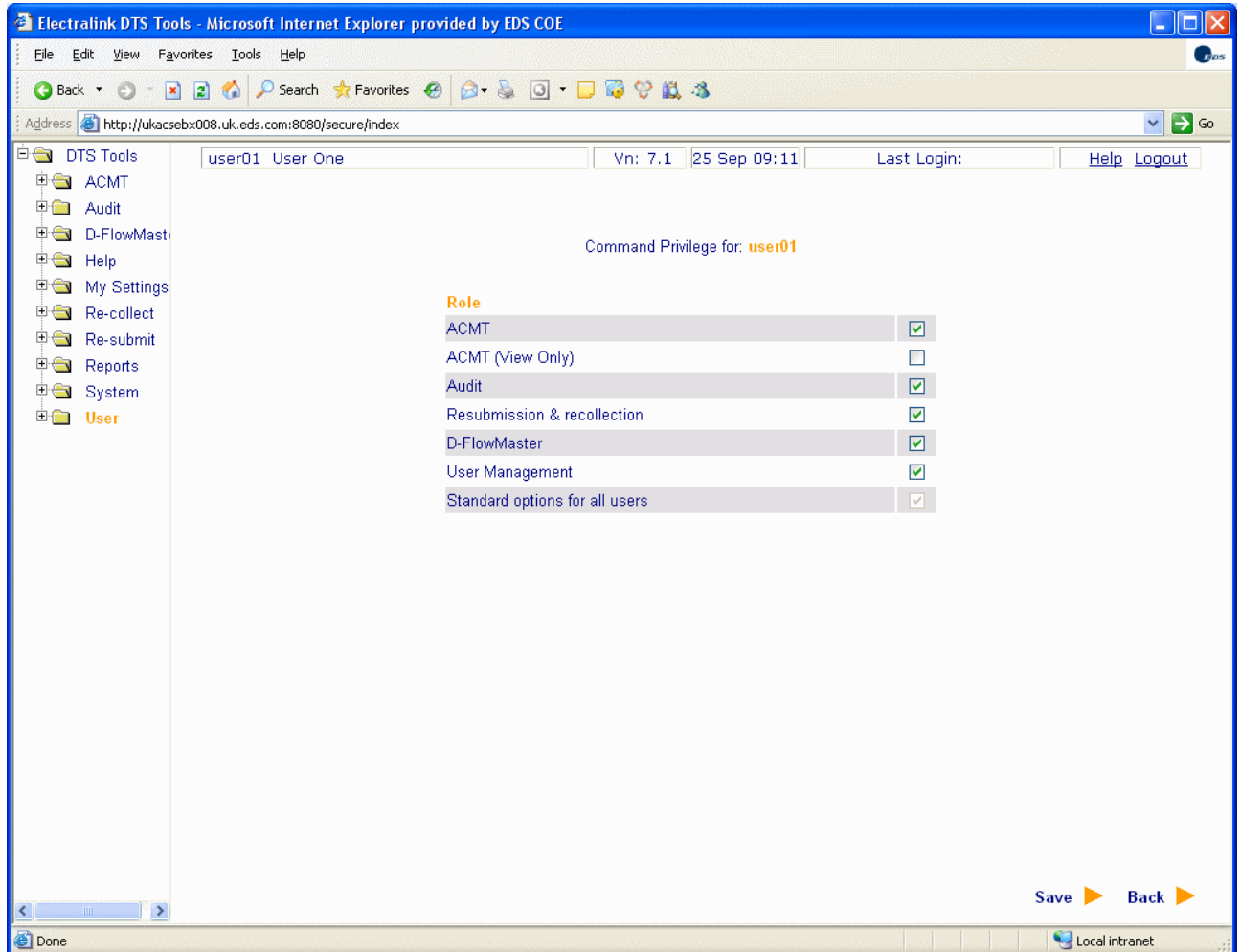


**Figure 2-5 User command privileges**

Permission to use a particular tool (command) is granted by checking the appropriate check-box. When all appropriate options have been selected, click on **Save** ► to make the changes permanent.

To exit the screen without making any changes, click on **Back** ►.

### 3.7.2 Data Access

After clicking on the  at the side of the first table on the user access levels display (see Defining User Access Levels above) the following page is displayed.

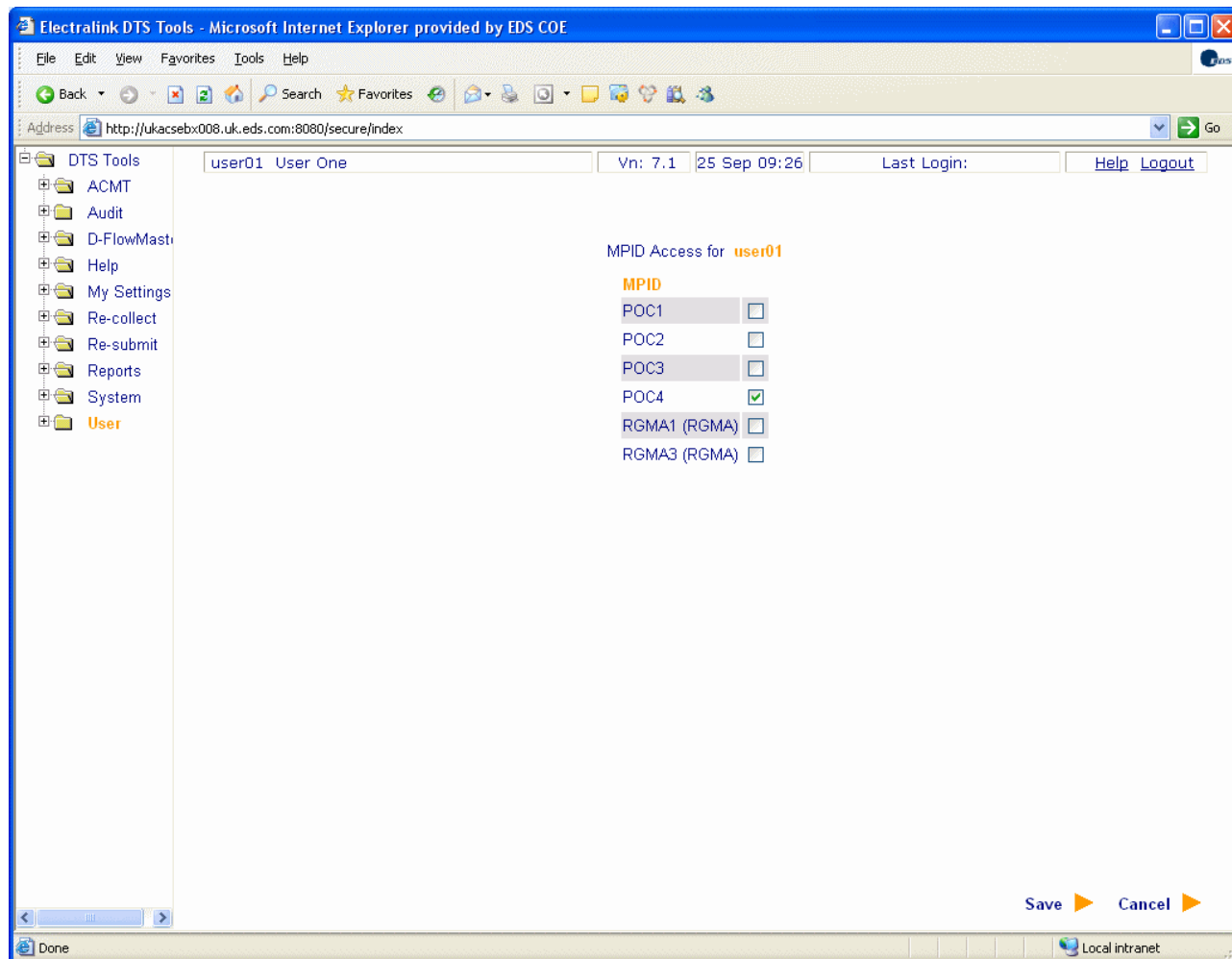


**Figure 2-6 MPID access privileges**

This display lists all the MPIDs that the user may be granted access to (i.e. the list of MPIDs your user group has been granted access to). Access is granted to MPIDs that are checked.

When you have granted access to the appropriate set of MPIDS for this user, click on **Save** ► to make the changes permanent.

To exit the screen without making any changes, click on **Cancel** ►.

After clicking on the  at the side of the second table on the user access levels display (see Defining User Access Levels above) the following page is displayed.

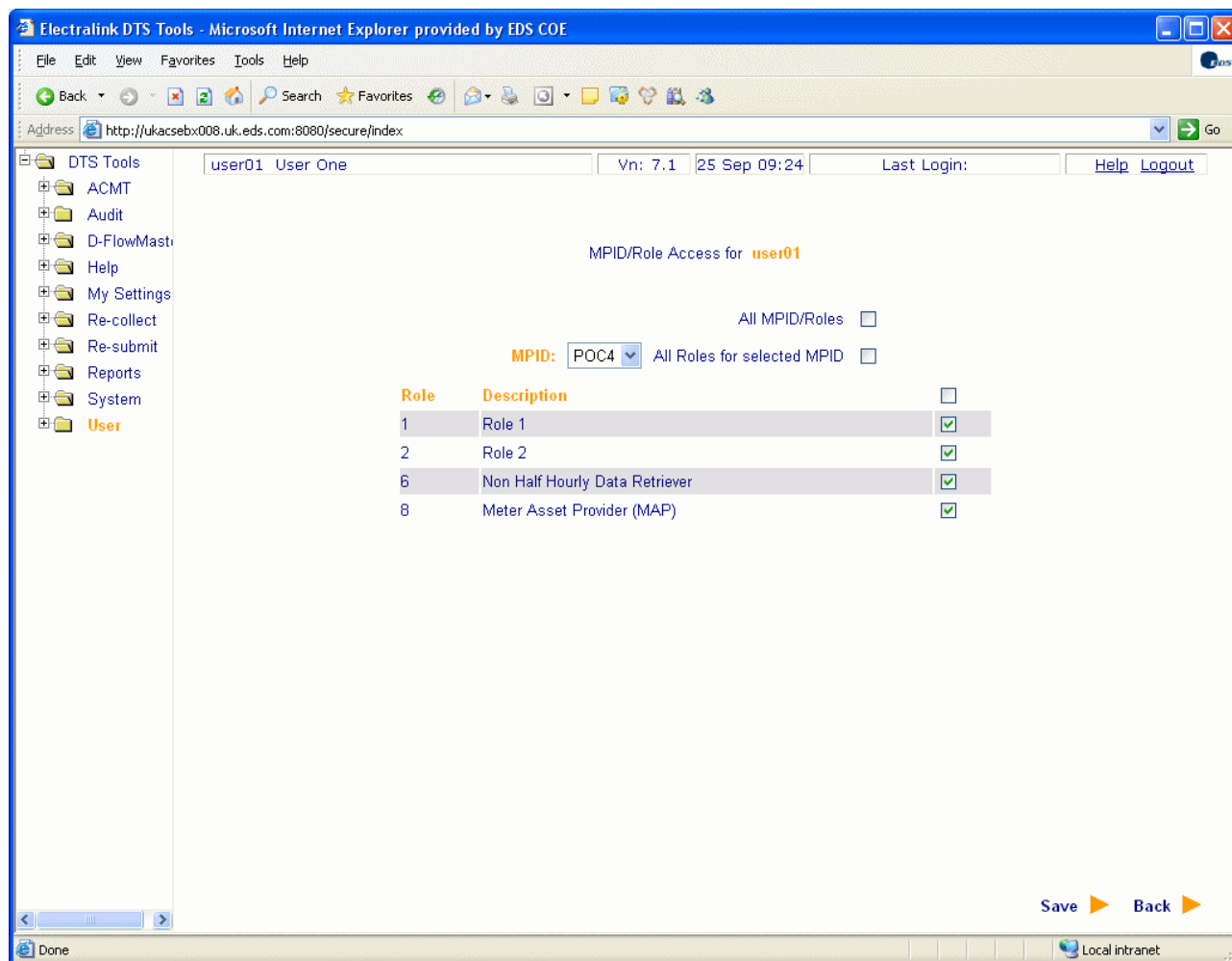


**Figure 2-7 Role access privileges**

This display lists all the Roles that the user may be granted access to. Only Roles associated with one of the MPIDs granted to the user are displayed. To view Roles for another of the MPIDs granted to the user, select it from the drop-down list.

- To grant/deny access to Roles for an MPID, check/uncheck the appropriate checkbox alongside the Role description.
- To grant access to all Roles associated with the MPID, check the 'All Roles for selected MPID' option. Note, this option is only available if the user group has been granted access to all roles for this, or all, MPIDs. If not available, the option will be greyed-out.
- To grant access to all Roles associated with all MPIDs to which the user has been granted access, check the 'All MPID/Roles' option. Note, this option is only available if the user group has been granted access to all Roles for all MPIDs the group has been granted access to. If not available, the option will be greyed-out.

After making changes to the Role access for an MPID, click on **Save** ► to make the changes permanent. After updating the database the page is re-displayed allowing Role access to be set-up for another MPID if necessary.

When Role access has been defined for all MPIDs, click on **Cancel** ► to return to the user access levels summary page and check that the access has been set correctly.

### 3.7.3 Gateway Access

After clicking on the  at the side of the third or fourth tables on the user access levels display (see Defining User Access Levels above) a page similar to the following is displayed:

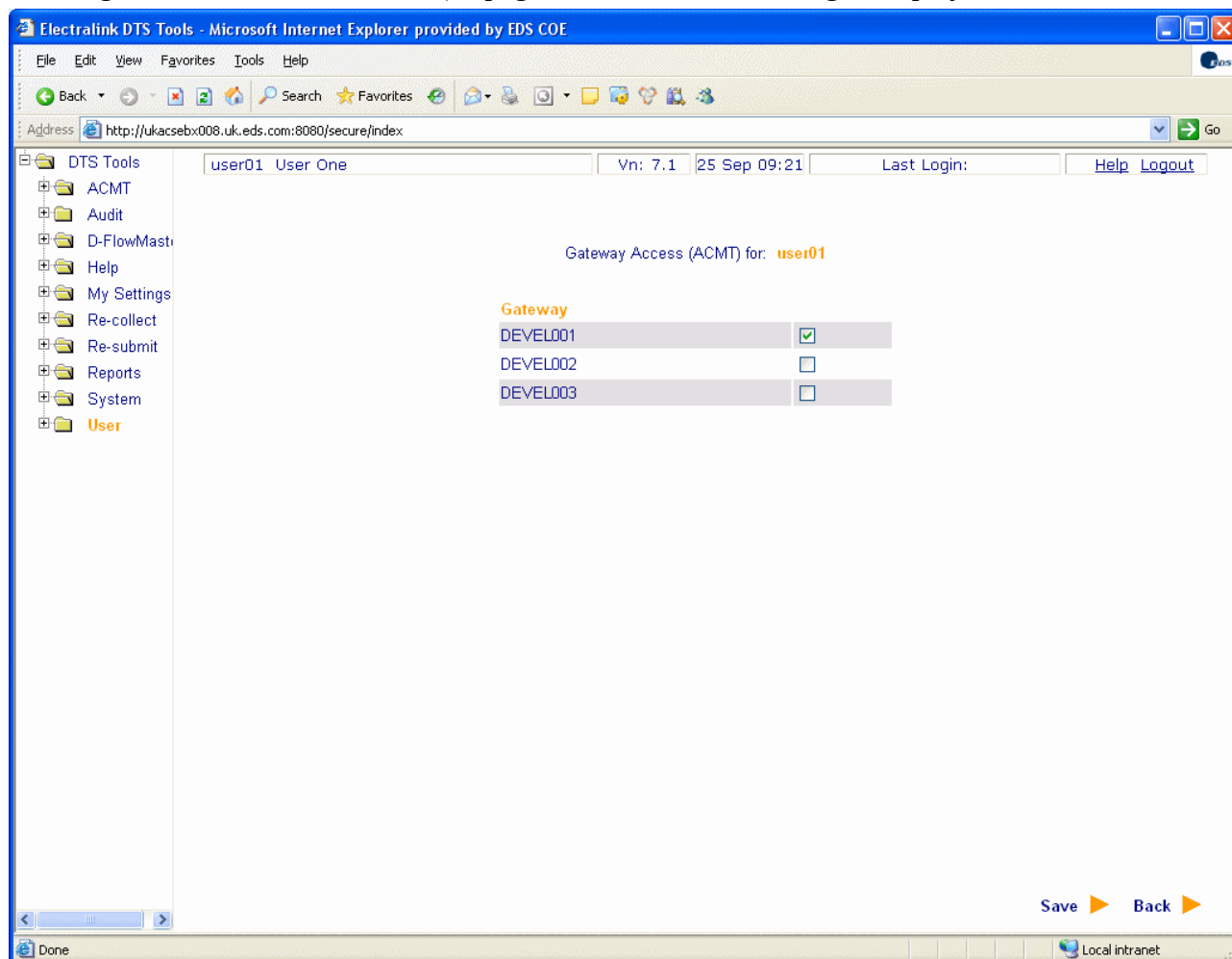


**Figure 2-8 Gateway access privileges**

This display shows which gateways the user can access in either the ACMT or Audit (inc. Re-submission & re-collection) tools. The title at the top of the page indicates which tool the access relates to.

Only gateways associated with MPID/Role combinations the user has access to are displayed.

Grant/deny access by checking/un-checking the relevant checkboxes.

When you have granted access to the appropriate set gateways for this user, click on **Save**  to make the changes permanent.

To exit the screen without making any changes, click on **Back** .

### 3.8 FLOW ACCESS

After clicking the  button at the side of the fifth table on the user access levels display (see Defining User Access Levels above) the following page is displayed:

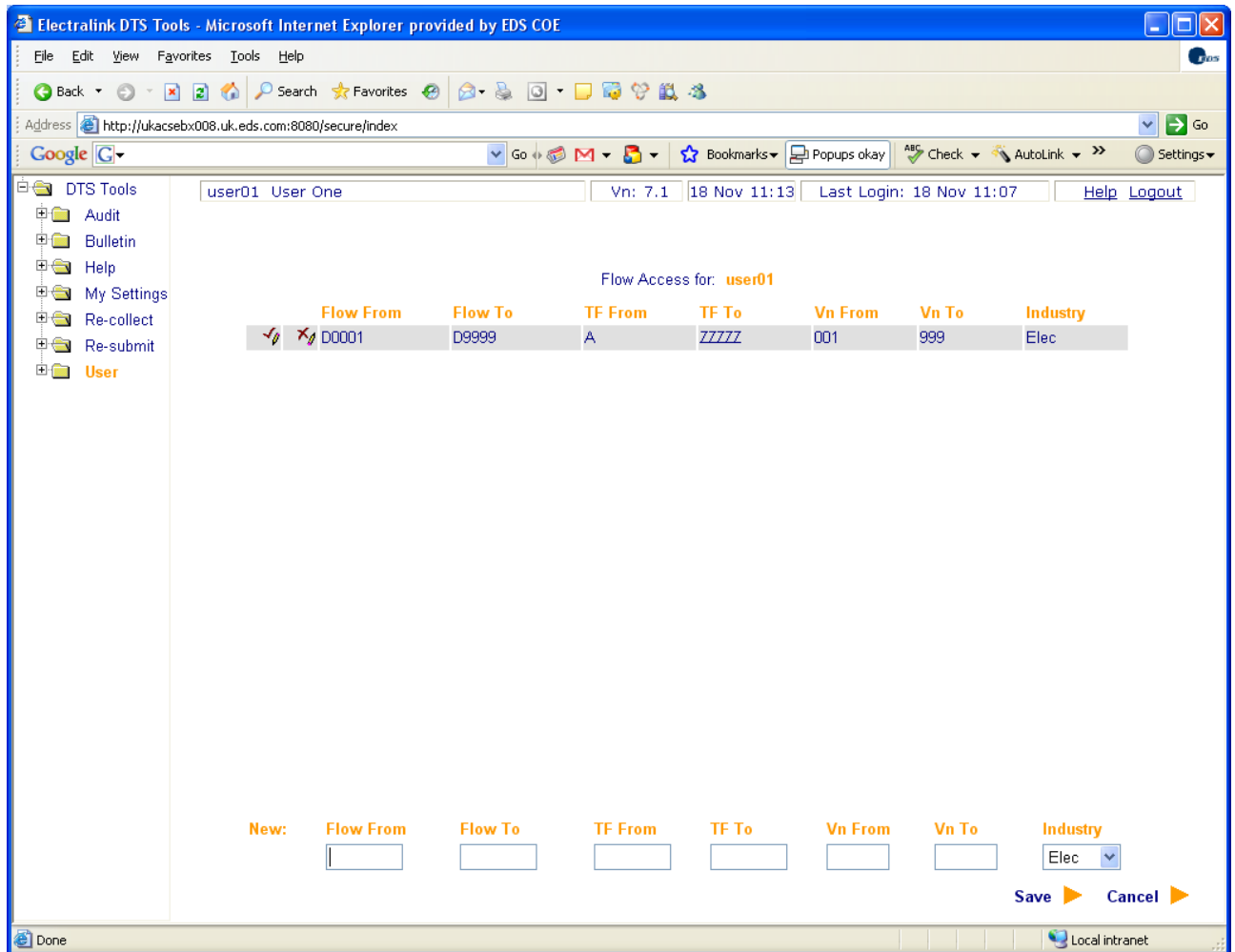


**Figure 2-9 Flow access privileges**

The data entry fields at the foot of the display only appear when creating a new range of accessible flows or editing an existing range.

From this page you may:

- Click the **New** button at the foot of the display (not shown in the figure above) to create a new range.
- Click the  button at the left hand side of the range to edit an existing range.
- Click on the  button at the left hand side of the range to delete that range.

For a user to be able to view, create, modify or delete a route in the ACMT tool;

- the flow id must be alphabetically between **Flow from** and **Flow To**
- AND the test flag must be alphabetically between **TF From** and **TF To**
- AND the flow version number must be alphabetically between **Vn From** and **Vn To**
- AND the flow must be from the **Industry** catalogue of flows

...for **one** of the user's defined ranges of flows. The example shown in Figure 2-51 Flow access privileges, gives this user access to all flows defined in the DTC and EFD catalogues.

If, for example, you want to restrict a user to viewing, creating, modifying and deleting routes for flows between D0100 and D0150 (inclusive) that have a TR02 test flag you would set a single range as follows:

|                  |       |
|------------------|-------|
| <b>Flow from</b> | D0100 |
| <b>Flow To</b>   | D0150 |
| <b>TF From</b>   | TR02  |
| <b>TF To</b>     | TR02  |
| <b>Vn From</b>   | 001   |
| <b>Vn To</b>     | 999   |
| <b>Industry</b>  | Elec  |

## 4 AUTOMATED PASSWORD RESET FACILITY

It is a fact of life that you may, on occasion, forget your password. So that you are not unduly inconvenienced if you do, the system offers an automated password reset facility. To be able to use this facility, you must have previously registered an email address with the ElectraLink helpdesk. This email address plays a key part in the process. You must supply the registered email address when requesting a password reset and it is to this address that the system will send messages in support of the reset process.

### 4.1 PASSWORD RESET REQUEST

A password reset request is initiated by clicking on the 'Forgotten password? Click here' link on the login screen.

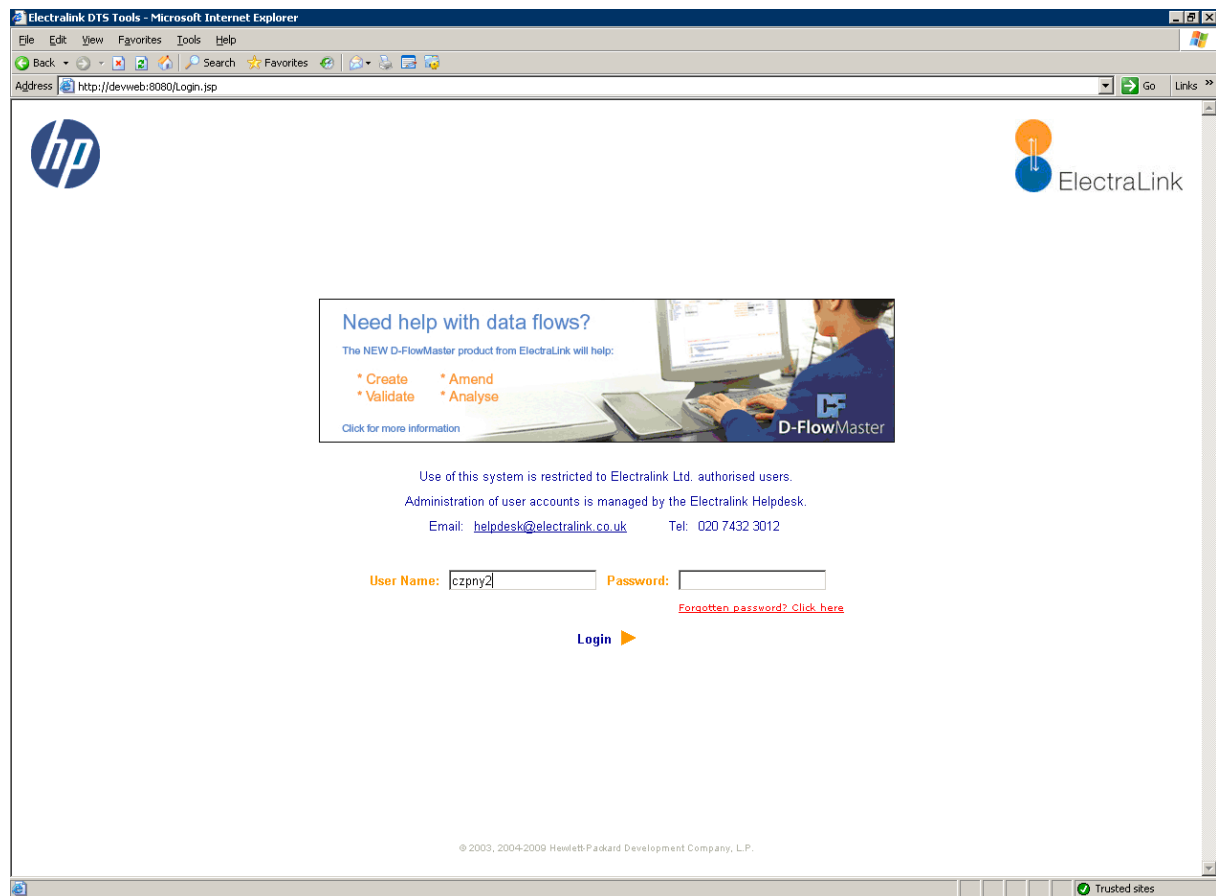


**Figure 2-1 Login screen**

This link takes you to the following password reset request screen:

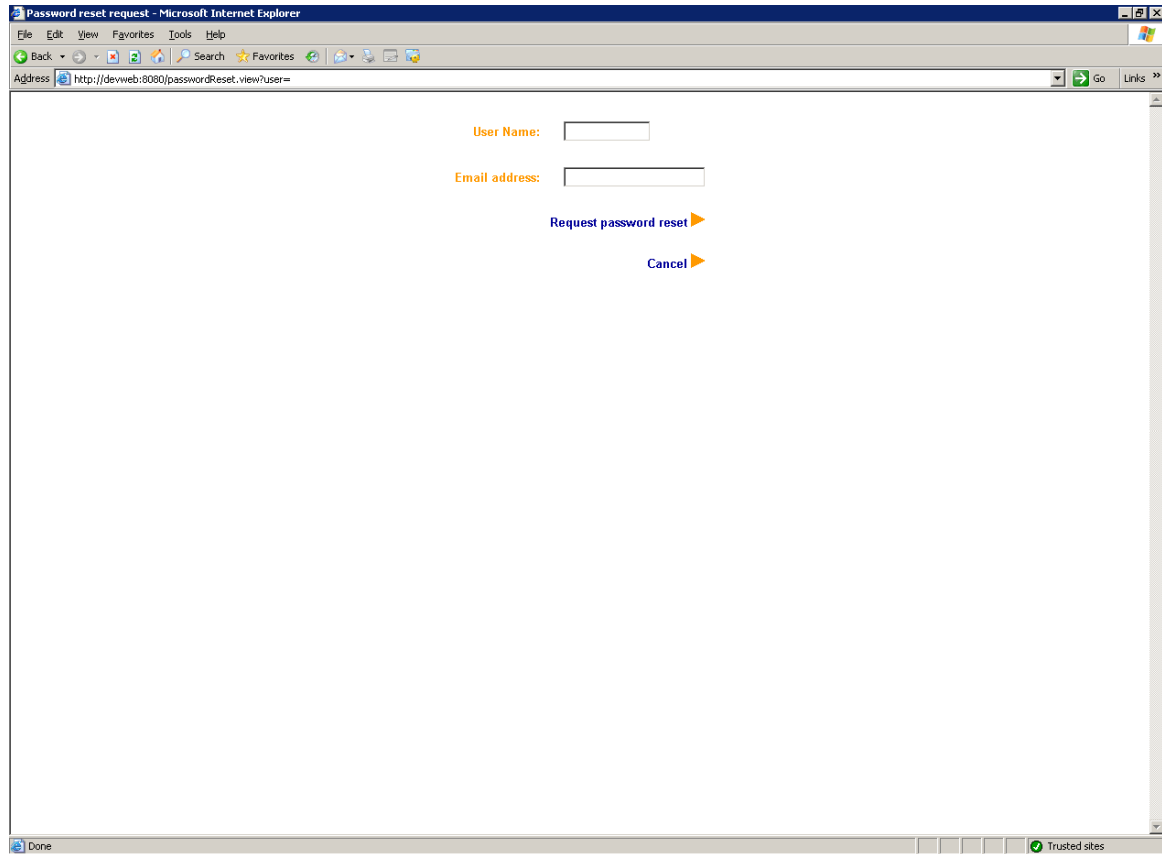


**Figure 2-2 Password reset request screen**

To request a password reset you must provide your WebTools user name and the email address previously registered for your user name. The user name will be pre-populated with any user name previously entered on the login screen, but can be changed if desired.

**This facility cannot be used unless you have previously registered an email address for your user account with the ElectraLink helpdesk.**

To complete the request you must click on the **Request password reset** button.

To abandon the process and return to the login screen, you should click the **Cancel** button.

If the user name you entered is not recognised by the system or the email address does not match the registered email address for your user name, an error message will be displayed below the corresponding data entry field.

Otherwise a screen will be displayed informing you that an email has been sent to the registered email address asking you to confirm that the password of the account should be reset. Examples of the screen and associated email are shown below:

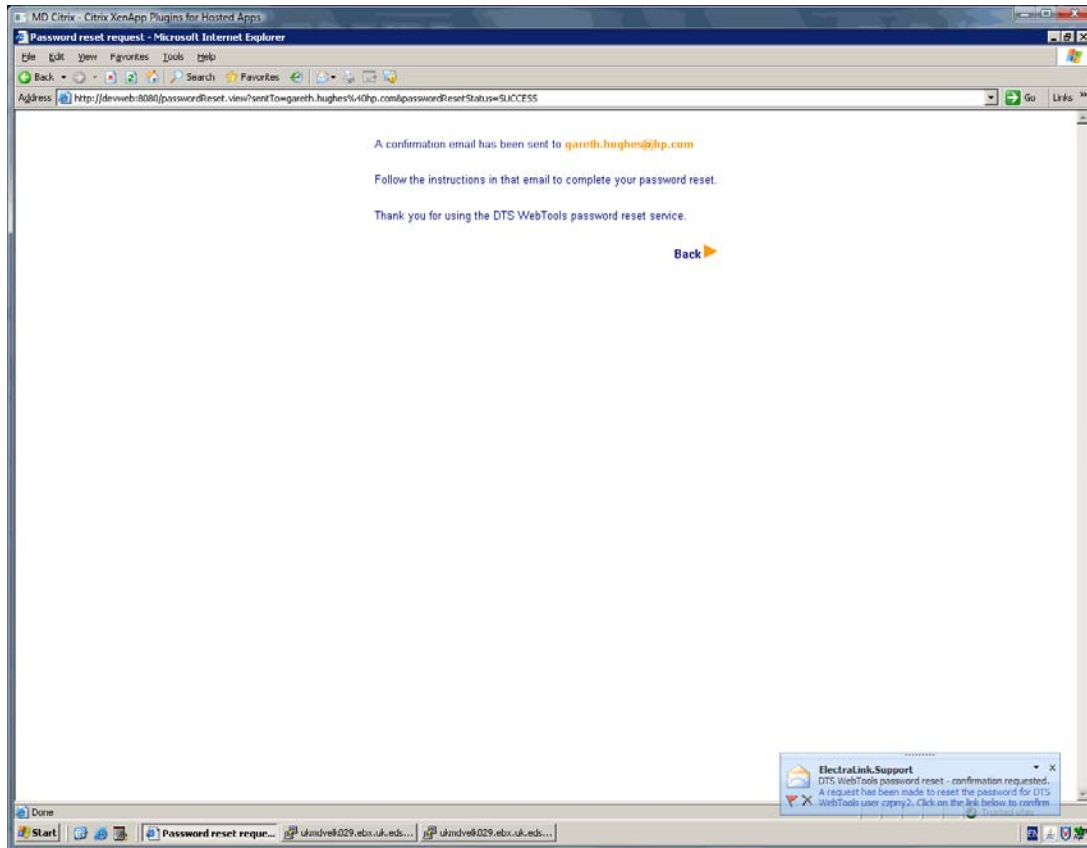


**Figure 2-3 Password reset request confirmation screen**

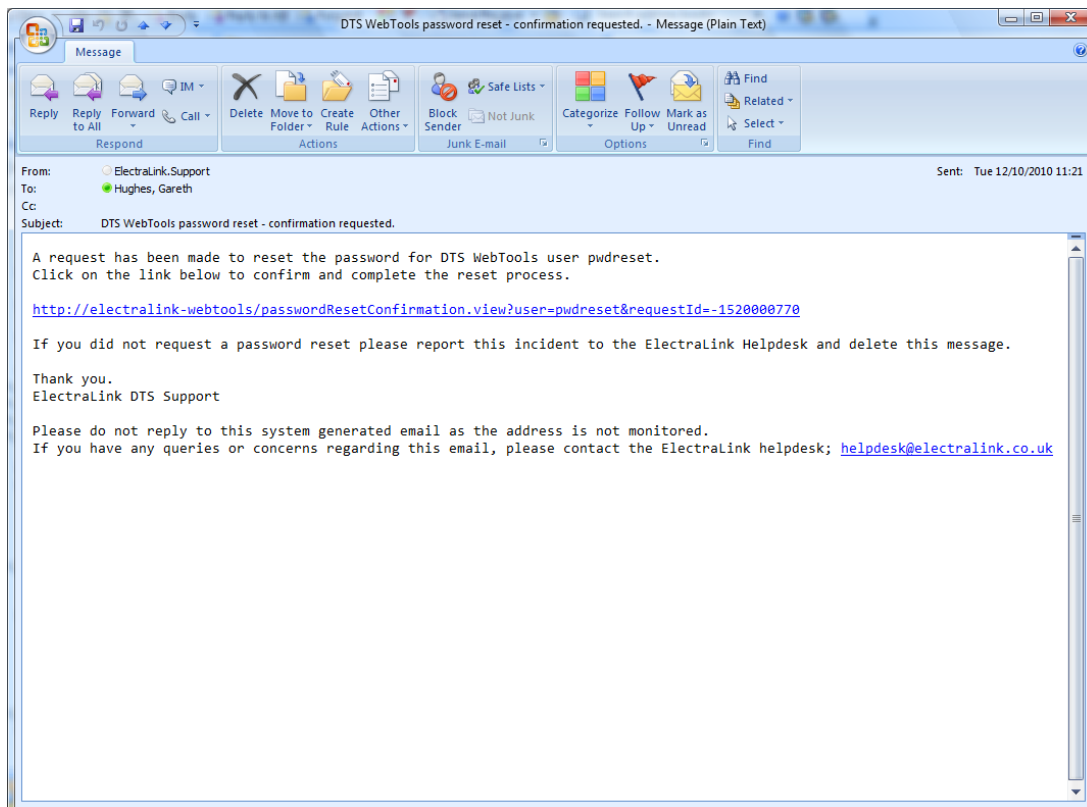


**Figure 2-4 Password reset request confirmation email**

To complete the password reset process you must click on the link (or cut and paste the link into the address bar of the browser you use to access WebTools) provided in the email.

This link will reset the password and display the new password on screen. An email will also be sent to the registered email address confirming the new password. Examples of the screen and email are given below:

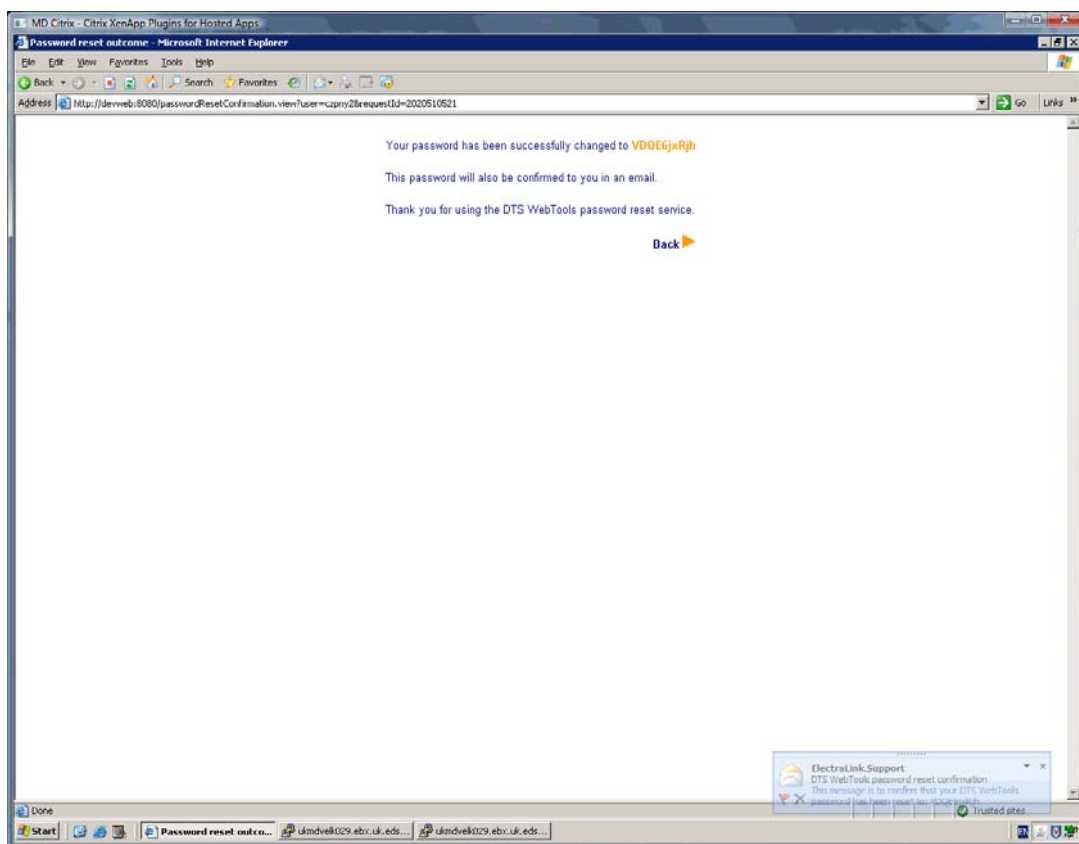


**Figure 2-5 Password reset confirmation screen**

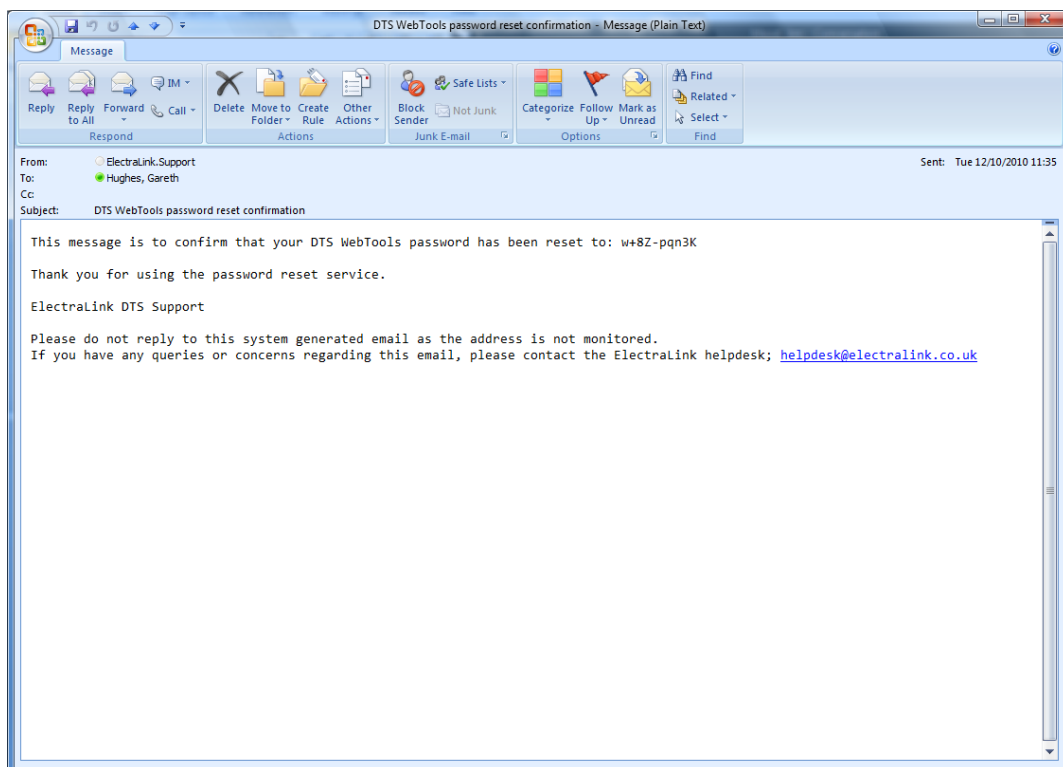


**Figure 2-6 Password reset confirmation email**

After you login to WebTools for the first time with this system generated password we strongly advise you to use the 'Change Password' facility to change the password to something you find more memorable.